Proof of Witness Presence: Blockchain Consensus for Augmented Democracy in Smart Cities

Evangelos Pournaras
ETH Zurich
Zurich, Switzerland
epournaras@ethz.ch

***Abstract*—Smart City data intensive urban environments are becoming highly complex and evolving by the digital transformation. Repositioning the democratic values of citizens' choices in these complex ecosystems has turned out to be imperative in an era of social media filter bubbles, fake news and opportunities for manipulating electoral results with such means. This paper introduces a new paradigm of augmented democracy that promises citizens who actively engage in a more informed decision-making integrated in public urban space. The proposed concept is inspired by a digital revive of the Ancient Agora of Greece, an arena of public discourse, a Polis where citizens assemble to actively deliberate and collectively decide about public matters. At the core of the proposed paradigm lies the concept of proving witness presence that makes decision-making subject of providing evidence and testifying for choices made in the physical space. This paper shows how proofs of witness presence can be made using blockchain consensus. It also shows how complex crowd-sensing decision-making processes can be designed with the Smart Agora platform and how real-time collective measurements can be performed in a fully decentralized and privacy-preserving way. An experimental testnet scenario on sustainable use of transport means is illustrated. The paramount role of dynamic consensus, self-governance and ethically aligned artificial intelligence in the augmented democracy paradigm is outlined.**

***Index Terms*—augmented democracy, Smart City, witness presence, consensus mechanism, blockchain, participation, crowd-sensing, decision-making, collective intelligence**

I. Introduction

Smart City urban environments co-evolve to complex informational ecosystems in which citizens' collective decisions have a tremendous impact on sustainable development. Choices about which transport mean to use to decrease noise levels or carbon emissions, which urban areas may require gentrification or new policies for improving safety are some examples in which decision-making turns out to be complex and dynamic [1]. It is apparent that the 4-year electoral agendas of political parties based on which they unfold their policies are either impractical or outdated for such urban ecosystems. Policy-making, participation and ultimately democracy requires a revisit and a digital transformation for the better of citizens.

Existing social media platforms, powered by citizens' personal data and centralized machine learning algorithms can isolate citizens via informational filters bubbles and manipulate them using fake information [2], [3]. Citizens often feel powerless to influence public matters and, beyond elections, there is no established channel for their voice to be heard in centers of decision-making [4]. Despite the technological capabilities to engage wisdom of the crowd for decision-making, decisions remain to a high extent top-down and political actions do not always align with electoral political agendas [5]. The rise of populism, extremism and electoral manipulations showcase the risks of democratic values in decay.

To address these challenges a new digital paradigm of augmented democracy is introduced to empower a more informed, engaging and responsible decision-making integrated to public urban space, where the decisions have a direct impact. In this sense, augmented democracy is envisioned as a digital revive of the Ancient Agora of Athens, a public assembly of citizens for discourse, deliberation and collective decisions-making. Witness presence has been so far the missing required value in digital democratic processes: the act of intervening and testifying about real-world as well as the undertaking of responsibility for these actions. For instance, making the rating of traffic congestion at different streets conditional to secure digital evidence about the citizen's location and speed records at these streets is an example of proving witness presence.

The envisioned scenario is the following: Citizens navigate over several urban points of interest with augmented information. They can make informed choices by proving witness presence in one of these points. They can also access live updates about the collective choices made by other citizens in relevant points of interests. This paper shows how this scenario can be made feasible and viable using secure, privacy-preserving and decentralized information systems, e.g. blockchain consensus, as well as crypto-economic design principles to incentivize participation and engagement. The proposed solution consists of the three following pillars: (i) *participatory crowd-sensing*, (ii) *proof of witness presence* and (iii) *real-time collective measurements*. Despite the complexity and ambition level of the proposed endeavor, this paper illustrates a first prototyped testnet scenario that integrates and demonstrates all three pillars. The role that dynamic consensus, self-governance and artificial intelligence play in the proposed augmented democracy paradigm is discussed.

Compared to related initiatives such as online petition/voting systems, the proposed augmented democracy paradigm fundamentally differs in the following aspects: it is not limited to long-term decision-making (non-real-time), it better integrates into the daily life of citizens as well as the public space, where a more informed decision can made. In summary, the contributions of this paper are outlined as follows:

- A new three-tier paradigm of augmented democracy in Smart Cities.
- The Smart Agora crowd-sensing platform for modeling complex crowd-sensing scenarios of augmented decision-making.
- The concept of 'proof of witness presence' for blockchain consensus.
- A review of blockchain-based approaches for proof of location.
- The concept of encapsulation in collective measurements that determines the point of interest from which data are aggregated.
- A working prototype of the augmented democracy paradigm meeting some minimal requirements for a first proof of concept.

This paper is outlined as follows: Section II introduces the vision and challenges of the augmented democracy paradigm that consists of three pillars. The first pillar of participatory crowd-sensing is illustrated in Section III. The concept of proving witness presence is introduced in Section IV that is the second pillar of the proposed paradigm. The third pillar of real-time collective measurements is illustrated in Section V. A proof of concept with an experimental testnet scenario is outlined in Section VI. Section VII discusses dynamic consensus and self-governance as well as the role of artificial intelligence in the introduced augmented democracy paradigm. Finally, Section VIII concludes this paper and outlines future work.

II. Augmented Democracy: Vision and Challenges

This paper envisions a digital revive of the ancient *agora* of Athens, a public cyber-physical arena of discourse, where citizens actively assemble, deliberate and engage in informed collective decision-making about a wide range of complex public matters. The scenario envisioned is the following: Individual citizens, regional communities or policy makers crowd-source complex decision-making processes augmented in Smart Cities, for instance, decide how to better integrate immigrants, how to improve public safety or transport means, how to deal with gentrification and others. Such processes are designed to encourage or even enforce a more informed and participatory decision-making to improve individual/collective awareness and the quality of decision outcomes. In practice this means that a citizen with a community mandate to participate in a collective decision-making process uses a smart phone and navigates in the urban environment to visit or discover *points of interests* with augmented information. For instance, after a natural disaster, i.e. flooding, earthquake, etc., citizens can rate the severity of damages at different locations to orchestrate mitigation actions more effectively. Citizens have a saying, an informed one, backed up by evidence of *witness presence* in the cyber-physical space of Smart Cities. Witness presence is an added value on citizens' decision-making created at a *certain location*, at *certain time* with a *certain situation awareness* when performing a *certain action*. Such evidence-based collective decision-making process introduces highly contextualized spatio-temporal data, whose aggregation creates a live pulse of the city, a public good created by citizens, for citizens. For instance, live updates about the severity of damages in certain areas can engage remote volunteers for support or act as warning signals for civilians to avoid these areas and protect their life.

Such a scenario of a direct augmented democracy in Smart Cities requires data-intensive information systems playing a key role for the viability of this challenging endeavor. A centralized design for these critical systems can pose several undermining risks: (i) Existing centrally managed online social media, along with traditional media, are often carriers of unaccountable and uncredible information that is a result of nudging and spreading of fake news [2], [3]. The damage in the participation level and trust of citizens on democratic processes, such as elections and referendums, can be unprecedented [6], [7]. (ii) The most prominent global localization service, the GPS, is centrally controlled, it has several security and privacy vulnerabilities, i.e. spoofing and jamming [8], it is not accurate enough and has restricted coverage, e.g. indoor localization is not feasible [9]. (iii) Collective measurements and awareness via Big Data analytics rely on trusted third parties that are single point of failure. They usually collect and store personal sensitive data and as a result profiling and discriminatory actions over citizens become feasible.

This paper claims that in principle any digital democracy paradigm cannot remain viable in the long term unless the management of information systems is democratized. As democracies cannot properly function in the long term with benevolent totalitarian forces, similarly, centralized information systems, however well they perform and simple to manage, they can always be subject of manipulation and misuse.

The positioning of this paper is that decentralized information systems, particularly distributed ledgers, consensus mechanisms and crypto-economic models, can by designed to support a more informed and participatory collective decision-making as shown within the three pillars of Figure 1. This is possible by introducing the concept of *witness presence* as a consensus model for verifying location and situation awareness of collective decision-making in Smart Cities.

The rest of this paper illustrates each of the three pillars in the proposed framework of augmented democracy.

III. Participatory Crowd-sensing

At the foundations of the framework lies the award-winning[1] platform of Smart Agora, a pillar that empowers citizens to (i) visually design and crowd-source complex decision-making processes augmented in the urban environment as well as (ii) make more informed decisions by witnessing the urban

[1]Smart Agora has been part of the Empower Polis project that won the 1st prize at the ETH Policy Challenge: http://www.policychallenge.ch (last accessed: April 2019).

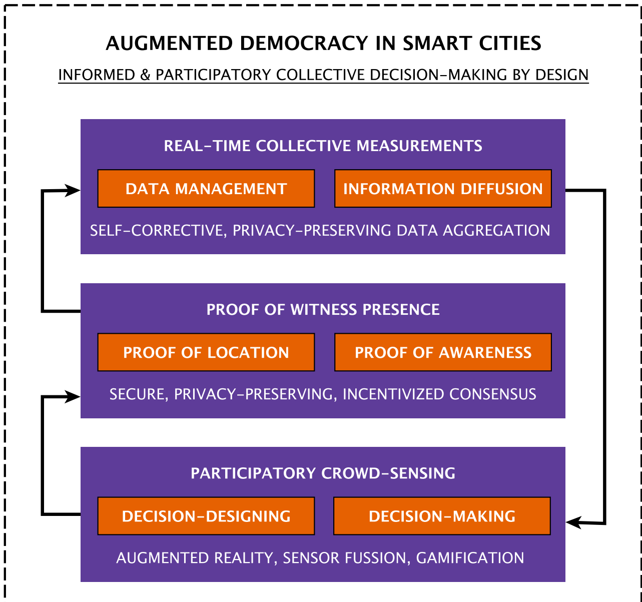


Figure 1: An augmented democracy paradigm for Smart Cities consisting of three pillars: (i) Crowd-sensing is performed within participatory witness presence scenarios of augmented reality in public spaces. (ii) Proof of witness presence is performed by securely verifying the location and the situation awareness of citizens without revealing privacy-sensitive information. (iii) Real-time and privacy-preserving collective measurements are performed, subject of witness presence.

environment for which decisions are made. Figure 2 outlines how an augmented democracy project is modeled[2].

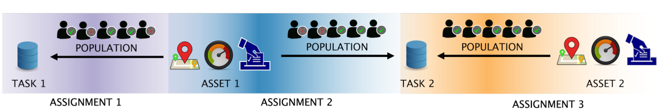
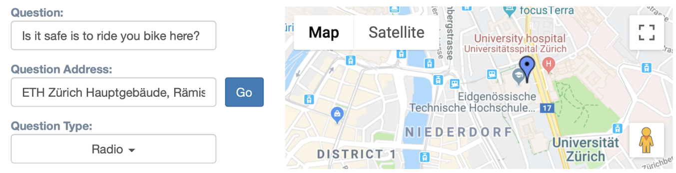
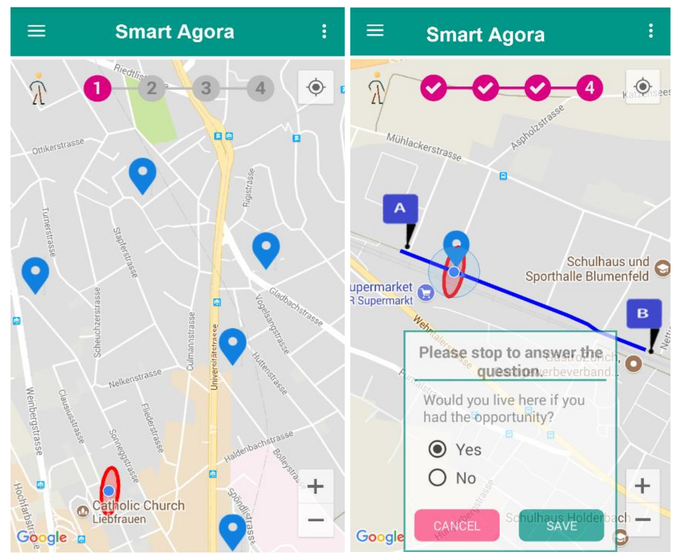


Figure 2: Modeling a crowd-sensing project with Smart Agora. A *project* consists of one or more *assets*, *tasks*, and *assignments*. (i) An asset defines complex crowd-sensing processes and consists of configurations about the point of interests, the questions and the collected sensor data. (ii) A task stores and manages the collected citizens' data as defined by an asset. (iii) An assignment links together an asset and a task and launches the crowd-sensing process by selecting candidate citizens for participation.

Decision-making processes are designed in a visual and interactive way as follows: A number of *points of interest* are determined in an interactive map as shown in Figure 3a. Each point of interest hosts a number of questions[3] that citizens can answer on their smart phone if and only if they are localized nearby the point of interest (see Figure 3b). An ellipse [10] with configurable size is determined around each moving citizen. Localization is performed when a point of interest falls in the ellipse, triggering an event that prompts citizens to answer questions on their smart phone based on what they witness in the public urban space they are located that moment.



(a) Determining point of interests with augmented questions.



(b) The Smart Agora App

Figure 3: The Smart Agora software platform.

Points of interest can be given by an oracle, i.e. a policy maker running a specific voting campaign, or they can be crowd-sourced to communities based on crypro-economic incentive models. For instance, FOAM [11] relies on token curated registries [12], [13] that realize economic and reputation incentives for citizens to play the role of cartographers and contextualize crypto-spatial coordinates[4] with meta-information.

Each question as well as their possible answers can be incentivized with rewards in the form of different crypto-currencies, i.e. utility tokens used for a value exchange required to run and incentivize the augmented democracy paradigm. For instance, tokens created by a city council to incentivize participation in a crowd sensing project for improving the quality of public transport can be collected and used by citizens to purchase public transport tickets. Similarly parking away from crowded city centers can be incentivized

[2]The modeled entities follow the concept of Hive https://github.com/nytlabs/hive (last accessed: April 2019).

[3]Radio, checkbox, likert and text box questions are currently supported.

[4]On-chain and off-chain verifiable location information of FOAM consisting of a geohash and an Ethereum smart contract address. It can approximate resolution in one square meter that allows a maximum of 500 trillion unique addresses.

with tokens that can issue discounts in nearby shops. Sensor data can also be periodically collected and can be used for supporting the two pillars above, i.e. sensor fusion to prove claims of witness presence [14] or aggregation measurements over sensor data can be performed to increase collective awareness [15].

A decision-making process can be designed in three *navigation modalities*: (i) *Arbitrary*–the points of interests can be arbitrary visited by citizens. Questions are always triggered whenever citizens visit a new point of interest. (ii) *Sequential*–A sequence is determined for visiting the points of interests. Only the questions of the next point of interest can be triggered, imposing in this way an order. (iii) *Interactive*–The next point of interest is determined by the answer of the citizen in the current point of interest. The latter modality can serve more complex decision-making processes as well as gamification scenarios.

IV. Proof of Witness Presence

Witness presence provides an added value in participatory decision-making [16], [17]. Witnessing public happenings and the complex urban environment of Smart Cities empowers a Polis of active citizens that can directly influence real-world by intervening and testifying instead of remaining passive spectators of a reality for which others decide, a limitation of current representative democracies. Ultimately, witness presence is about encouraging the taking of responsibility, a requirement for a viable democracy. While witness presence can be seen as a political statement, in the context of the proposed augmented democracy paradigm it is a highly complex techno-socio-economic problem: Proving of being present at a certain location, at a certain time with a certain situation awareness in order to perform certain actions, while having the incentive to participate. This section reviews blockchain consensus models for the digital and physical world, whose synthesis could shape a solid solution to this grand research challenge.

A. A review on proof of location

At the core of witness presence lies *proof of location* that is the secure verification of a citizen's location. It requires accurate estimation of distances or angles of signals exchanged between devices. These distances are calculated by measuring signal attenuation or signal propagation times. Techniques of the former, i.e. Received Signal Strength Indicator (RRSI) [18], are common but do not provide accurate estimates, while techniques of the latter, i.e. Time of Flight (ToF) with algorithms based on triangulation, trilateration or multilateration, require synchronized clocks to eliminate clock drifts of the oscillators [19]. For example, the Global Positioning System (GPS) relies on high-precision atomic clocks on satellites that synchronize with centralized master control stations on the ground. Recently, decentralized algorithms for Byzantine fault-tolerant clock synchronization have been studied [20]. These algorithms run by autonomous interactive wireless receivers and transmitters, i.e. beacons, that self-determine via their communication the geometry of their zone coverage without third parties. By reaching an agreement about a common time[5] specific locations can be accurately detected via trilateration [21].

The proof of location required for the proof of witness presence can be achieved with various trade-offs using one or more of the following infrastructures: (i) *GPS*, (ii) *mobile cellular network*, (iii) *low power wide area network* (LPWAN) and (iv) *peer-to-peer ad hoc (opportunistic) networks* consisting of several different Internet of Things devices such as smart phones, static beacons, wearables, wireless access points, etc. Table I summarizes a comparison of the blockchain-based approaches for proof of location.

On the one hand, GPS is a free service with planetary coverage and as such it can be easily used by the Smart Agora application for outdoor localization, as the current prototype supports. Similarly, GeoCoin relies on GPS for the location-based execution of smart contracts [9]. However, GPS is a single point of failure, it is highly susceptible to fraud, spoofing, jamming and cyber-attacks, it does not provide any proof of origin or authentication and therefore it is unreliable by itself to prove claims of locations. Moreover, GPS cannot provide indoor localization, it underperforms in high density urban environments, i.e. increased signal multipath, and its energy consumption is prohibitive for low-power devices. Despite these limitations, there is active research on building secure and privacy-preserving localization solutions based on GPS by introducing additional protocol and security mechanisms, for instance, crowd GPS-based active localization based on digital signatures and bulletin boards applied for tracking lost items [24], [25].

Mobile cellular network providers have been earlier proposed to act as oracles to submit positioning information to smart contracts that verify whether such positions are included into virtual borders referred to as *geofences* [22]. Such geofences are represented by location encoding systems, for instance, Geohash and S2, that are hierarchical, i.e. they can model different cells at different resolution level. A geofence can be used by a local community to self-regulate its (i) decision-making territory and (ii) crypto-economic activity resulting from the incentivized participation in decision-making. The former determines the validation territory of witness presence claims. The latter determines the geographic areas in which transactions are permitted with collected tokens. For instance, Platin aspires to support such crypto-currencies for humanitarian aid use cases [26]. To control transaction costs for the execution of smart contracts, localization can be performed with different schemes: at regular time or distance intervals, on demand or upon violation of a citizen's presence in a geofence. Localization via mobile cellular networks can only though take place within the covered area of the mobile operator and global coverage requires special roaming service and collaboration between different mobile network operators. An alternative approach to overcome this limitation is to allow cellular towers of any mobile network to provide secure loca-

[5]Not necessarily a UTC time unless some oracle information is used.

Table I: Blockchain-based approaches for proof of location.

Approaches	GPS [9]	Mobile Cellular Network [22]	LPWAN [11]	P2P Ad Hoc Networks [23]
Infrastructure-independent	No	No	No	Yes
Decentralization	Low	Low	Medium	High
Access	Open	Closed	Open	Open
Management	Governmental-level	Enterprise-level	Community-level	Self-organized
Disaster Resilience	Medium	Medium	Medium	High
Coverage Range	Global	National	Urban	Localized
Indoor Coverage	No	Yes	Yes	Yes

tion services for the blockchain. Such an approach is earlier introduced that involves cellular towers with a well defined location issuing location certificates and participating in proof of location mining. Trust is achieved using cryptographically signed IP packets [27].

An alternative infrastructure to the proprietary and closed networks of mobile operators is the use of Low Power Wide Area Networks that allow access to an unlicenced radio spectrum [28]. LPWAN provide the following alternative trade-offs: long range, low power operation at the expense of low data rate and high latency. For instance, The Things Network [29] builds a global open LoRaWAN network of 7231 gateways in 137 cities run by local self-organized communities providing extensive coverage in urban environments. FOAM intends to use this decentralized open infrastructure for secure location verification enforced by smart contract safety deposits. Proof of location is performed within a *zone* (community operator) defined by at least four *zone authorities* (radio gateways) each managing a number of *zone anchors* (radio beacons). A zone anchor is a device with a radio transmitter, a local clock and a public key. It is capable to engage in a Byzantine fault-tolerant clock synchronization protocol [20]. Zone anchors mine triangulations and verify claims of presence via authentication certificates that are fraud proof. A zone authority is a node with an Internet connection that determines whether the zone anchors are in sync.

All of the above solutions among others [30], [31], [32] require additional special infrastructure. Mobile cellular networks and LPWAN may be unavailable or underperformimg in cases of natural disasters and unpredictable high-density mobility patters. In these scenarios, an alternative infrastructure-independent and decentralized approach is the use of peer-to-peer ad hoc (opportunistic) networks formed by self-organized citizens' devices running decentralized secure protocols based on blockchain proof of stake consensus mechanisms [23]. Proofs of location are performed between *witnesses* and a *prover*, whose Bluetooth interactions verify the identities of the involved devices as well as whether the location claims of each device are reachable within the radio coverage supported by the communication technology of the devices. Spatio-temporal mobility patterns of users may influence the verification process and additional measures of verification may be required, for instance, analysis of betweeness in pseudonym correlation graphs [33] or social tracking distance metrics [25]. Periodically changing the device identifiers according to a Poisson distribution prevents the reveal of real identities by observing location proof records [33].

B. *Situation awareness and proving witnessing*

A few blockchain approaches combine network-based with social-based proof of location [34], [26], [14]. For instance, on-chain location claims at Platin consist of a public key and a proof of correctness that in practice is the output of one out several locally executed algorithms that can validate location information based on the following three security pillars: (i) *sensor fusion*, (ii) *behavior over time* and (iii) *peer-to-peer witnessing*. Sensor fusion relies on multiple sources of sensor data, i.e. GPS, wireless access points, cell tower and Bluetooth oracles, for validation of location claims. Behavior over time reasons about any behavioral anomaly that indicates spoofing. Data-driven verification can be localized to preserve privacy by design and prevent turning proofs of witness presence to surveillance actions that can actually undermine and manipulate democratic processes [35]. Peer-to-peer witnessing using ad hoc opportunistic networks can be used as an additional counter-measure to testify for attackers that may replay sensor fusion or report fake behavior over time.

Proofs of witness presence verify the situation awareness required for a more informed collective decision-making. For instance, assume a crowd-sensing collective movement for a spatio-temporal safety assessment of bike riding in a city. Citizens rate the safety of different points of interests in the city based on which new data-driven policies can be designed to encourage the further safe use of bikes and the improvement of the infrastructure, i.e. new bike lanes. Making safety rating on the points of interest subject of proving witness presence can potentially improve the rating quality and as a result the effectiveness of a new designed policy. Beyond citizens proving their location, proving bike riding experience, on spot or elsewhere, indicates a situation awareness with an added value and a higher potential for a more effective policy. Verification can be performed on-chain or off-chain using witnesses, sensor fusion, i.e. analysis of GPS/accelerometer data, or even oracles, i.e. a bike sharing operator.

Other means to verify witness presence include the following: Contextual QR codes [36], challenge questions, puzzles and CAPTCHA-like tests [37], whose solutions require information mined at the point of interests. In addition, collaborative social challenges [38], [39] between citizens are means to introduce social proofs based on social psychology as well as community trust for protection against social engineering attacks [40]. Moreover, communities can also institutionalize their own digital witnesses based on privacy-preserving forensic techniques introduced in the context of blockchain [41], [42].

V. Real-time Collective Measurements

Real-time collective measurements are the aggregation of citizens' crowd-sensing data, e.g. decisions, made as a result of witness presence. The computation of aggregation functions, e.g. summation, mean, max, min standard deviation, are some examples of such collective measurements. They can be used as follows: (i) Citizens receive real-time crowd-sensing information. (ii) A collective awareness is built that is used as live feedback for future crowd-sensing decisions, i.e. the feedback loop in Figure 1. (iii) Put into action or enforce collective decisions on the participating citizens. (iv) Collective measurements may encourage or discourage witness presence, for instance, a warning system that guides authorities to mitigate a physical disaster in certain points of interest, while citizens are instructed to avoid dangerous ones.

A transparent and reliable system for collective measurements is paramount for building collective awareness and trust among citizens, both required for a viable augmented democracy paradigm. Existing centralized polls and social media often fail to provide reliable and trustworthy information and are often subject of citizens' profiling over collected personal data, nudging and political manipulation [43], [2], [3]. Instead, the computations required for aggregation can be crowd-sourced to citizens using their personal devices or computational resources of communities in a similar fashion as the diaspora* social network [44]. Although decentralized computations for aggregation are more privacy-preserving by design using differential privacy and homomorphic encryption techniques, their accuracy requires significant self-adaptations to cope with the following: (i) continuous data streams as a result of changes in decision-making, (ii) a varying spatio-temporal participation level as well as (iii) (Byzantine) failures.

The relevance of these challenges in the augmented democracy paradigm is the following: Citizens revisiting a point of interest in the future may reevaluate an urban quality triggering recomputations of the aggregation functions to reflect changes on the input crowd-sensing data. The decision of a citizen reflects on the aggregation functions as long as witness presence is proved. If witness presence cannot be verified anymore, corrective rollback operations on the aggregation functions are performed to reflect the latest status of participation. Similarly, any failure that cannot guarantee a correct execution of the aggregation protocol shall be treated as a failure to verify witness presence and therefore, corrective operations with rollback operations are performed in this case as well. In summary: *collective measurements provide a live pulse of a crowd, whose localization at points of interest is verified for witness presence*.

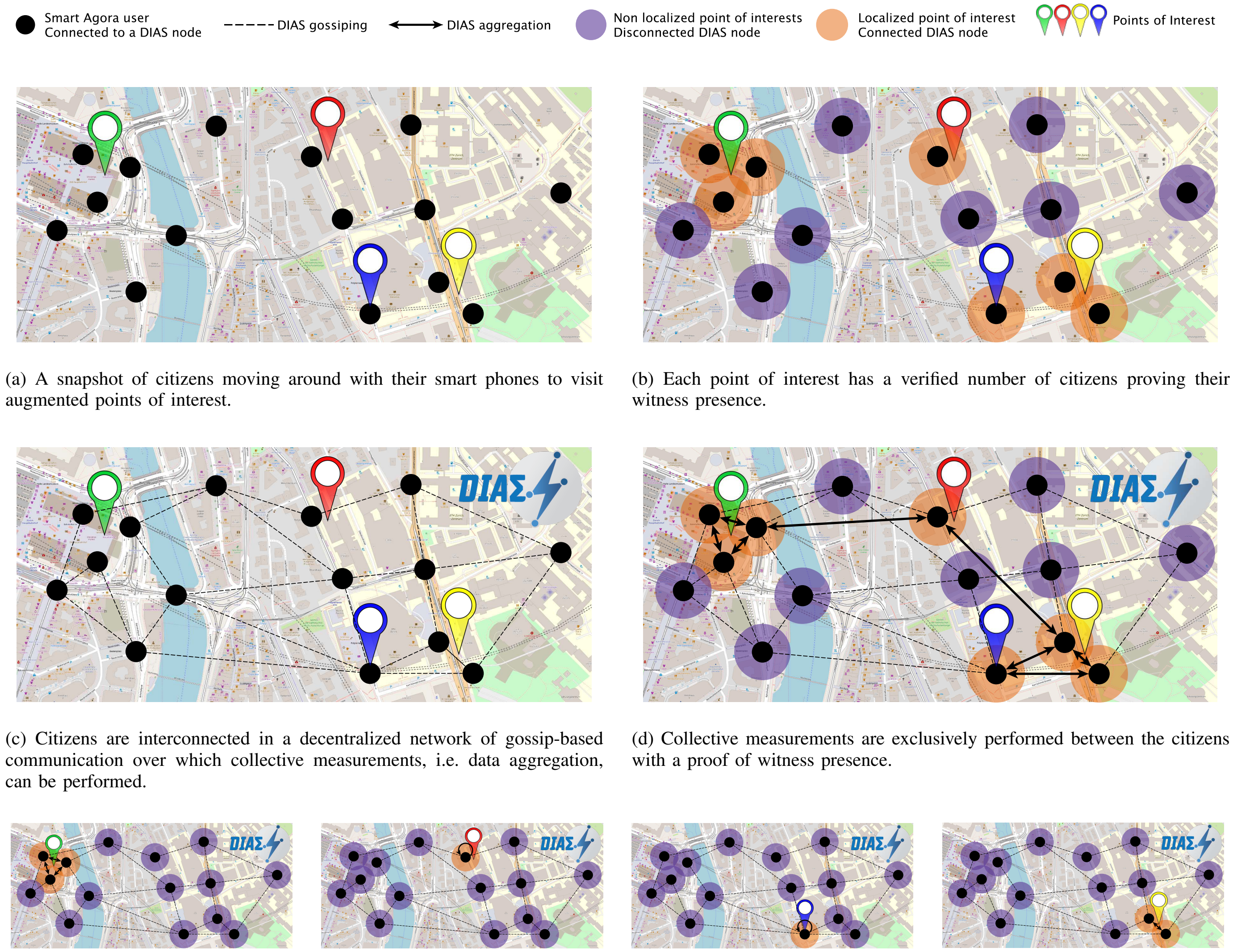
A possible feasible decentralized approach to realize this ambitious concept is the use of DIAS, the *Dynamic Intelligent Aggregation Service* [45]. DIAS is a network of interconnected agents deployed in citizens' personal devices or in computational resources of regional communities around points of interest. Agents perform a gossip-based communication to disseminate crowd-sensing data used as input in aggregation functions computed locally by each agent. The agents of DIAS are self-adaptive and can update the aggregates in an automated way when input data change as well as when agents join, leave or fail. They have this capability by a privacy-preserving reasoning based on historic data. Reasoning relies on a distributed memory system that consists of probabilistic data structures, the Bloom filters. In simple words and practical terms, the memory system can reason whether the evaluation of an urban quality by a citizen has changed at a point of interest. It can also reason on whether a citizen visits again or leaves a point of interest. Further technical information about DIAS is out of the scope of this paper and readers are referred to earlier work [45], [46], [47].

The augmented democracy paradigm can run in two different encapsulations that determine the relation between the collective measurements, i.e. a DIAS aggregation network, and a point of interest: (i) *one-to-many* or (ii) *one-to-one*.

In the one-to-many encapsulation, aggregation functions receive the input data of citizens, who prove witness presence in one out of several possible points of interest. In other words, a logical disjunction (OR) is introduced to the participation in the collective measurements by requiring the proof of witness presence at one possible point of interest. This encapsulation is relevant for federated democratic processes of regional communities, for instance collective decision-making in the spatial context of multiple university campuses, i.e. an 'eduroam' version of augmented democracy. Figure 4a-4d illustrate the augmented democracy paradigm in the one-to-many encapsulation.

In the one-to-one encapsulation, aggregation functions receive citizens' input data by proving witness presence at a certain point of interest. This encapsulation is relevant for local regional communities that use their own computational resources to run their own collective measurements and make them available to their local citizens. Figure 4e-4h shows an example of the one-to-one modality. For each point of interest, aggregation is restricted between the localized citizens proving witness presence.

The two proposed encapsulations are not the only options. Collective measurements can be subject of a more complex witness presence logic than the one of the two proposed exemplary encapsulations. For instance, collective measurements can run by two DIAS networks aggregating crowd-sensing data at point of interests corresponding to (i) tram stations and (ii) bus stations respectively.



(a) A snapshot of citizens moving around with their smart phones to visit augmented points of interest.

(b) Each point of interest has a verified number of citizens proving their witness presence.

(c) Citizens are interconnected in a decentralized network of gossip-based communication over which collective measurements, i.e. data aggregation, can be performed.

(d) Collective measurements are exclusively performed between the citizens with a proof of witness presence.

(e) Regional community A

(f) Regional community B

(g) Regional community C

(h) Regional community D

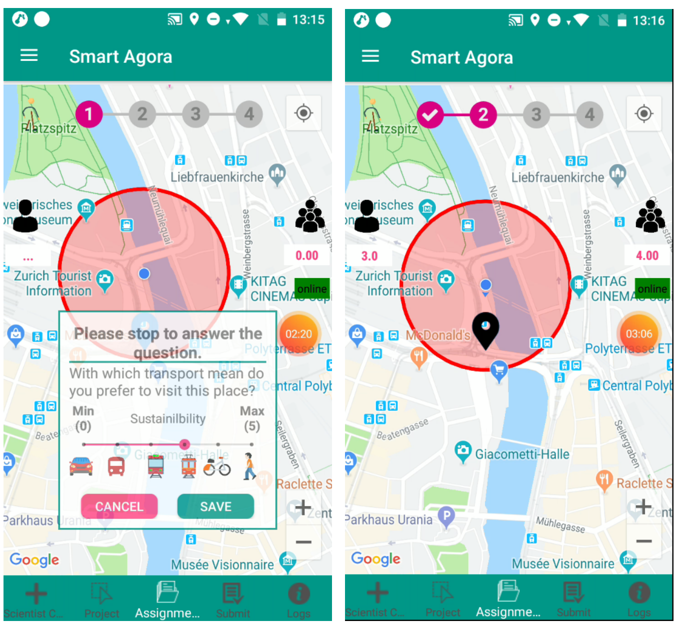
Figure 4: An illustration of the augmented democracy paradigm. **One-to-many encapsulation in Figure 4a-4d**: Collective measurements are performed by proving witness presence at one out of several possible points of interest. **One-to-one encapsulation in Figure 4e-4h**: multiple localized collective measurements are performed by proving witness presence at a certain point of interest.

VI. Experimental Testnet Scenario

Evaluating the end-to-end integrated functionality of the whole augmented democracy paradigm illustrated in Section **??** is a challenging endeavor. This requires a rigorous extensive evaluation of each proposed pillar that is subject of active ongoing work [48]. Such detailed evaluation does not fall within the scope and objectives of this paper. To overcome the aforementioned challenge and come with a very first proof of concept, a simple yet fully-fleshed experimental testnet scenario is designed with the following requirements: (i) A realistic Smart City use case for participatory crowd-sensing. (ii) Proof of witness presence in two points of interest based on GPS. (iii) Real-time collective measurements in one-to-many encapsulation over a small crowd of test users with different realistic mobility patterns.

A testnet scenario on sustainable transport usage is introduced to address the first requirement. The testnet scenario ran for about one hour on 3.6.2019 between 13:00-14:00 in Zurich. The goal of the testnet scenario is to assess the preferred transport mean with which citizens visit a place they witness. Such a use case is very relevant to transport engineers, who work with travel diaries. While travel diaries are modeled based on traditional, costly and infrequent survey questions, the pervasiveness of the Internet of Things promises new opportunities for more realistic and real-time data collection based on which future traffic flow models can rely on [49], [50]. Similarly, city councils can establish new policies and incentives for citizens to make use of more sustainable transport means. This use case assumes a linear model of sustainability over six transport means: 0. *Car*, 1. *Bus*, 2. *Train*, 3. *Tram*, 4. *Bike*, 5. *Walking*. These transport means are common in Zurich and usually a destination can be reached fast with several different transport means. Car comes with the minimum sustainability value of zero, while walking comes with the maximum sustainability of 5. Although this linear model is an oversimplification over several involved sustainability aspects such as environment, health, safety, social and other, it is intuitive and straightforward to engage test users as well as interpretable. Therefore, the purpose of the use case is to serve the realism of the testnet scenario rather than collecting use case data for a rigorous analysis.

The second requirement is met by designing a decision-making process in Smart Agora for the testnet scenario. The test users make a choice via a likert scale question that pops up in the Smart Agora app when they are localized at a point of interest as shown in Figure 5a. Such a question is part of six crowd-sensing Smart Agora assets created for six test users, who are equally split into two groups.



(a) Localization. (b) Aggregation.

Figure 5: Assessing the preferred transport mean to reach a witnessed point of interest in terms of sustainability. Localization triggers a question followed by live collective measuments received from other test users localized to other points of interests.

To meet the third requirement, each crowd-sensing asset is designed in the sequential navigational modality with two points of interest traversed in reversed order among the two groups to assess the one-to-many encapsulation of the DIAS collective measurements, i.e. choices of test users are aggregated in real-time from different remote points of interest. Figure 6 illustrates the designed experimental scenario. Note that the depicted walking path is the calculated Google Maps path rather than the one that test users followed[6]. The actual traces within the localization circles collected with Smart Agora are shown in Figure 8.

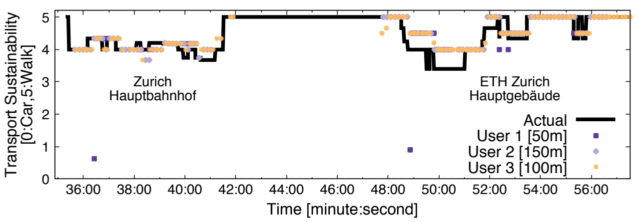
Figure 6: An overview of the testnet scenario: Two groups each with three test users visit in reversed order the two point of interests of (i) Zurich Hauptbahnhof and (ii) ETH Zurich Hauptgebaüde starting from Stampfenbachstrasse 48, 8092, Zurich, where the Chair of Computational Social Science of ETH Zurich is situated. Group 1 (Orange) visits first Zurich Hauptbahnhof and Group 2 (purple) visits first ETH Zurich Hauptgebaüde. Each unique localization to one of the points of interest triggers for a test user a question for assessing sustainable transport usage. While this test user remains localized, live collective measurements among all other localized test users are received. The three nested circles around each point of interest visualize the three different ranges of localization that each group member has: 50, 100 and 150 meters.

To make sure that multiple test users are localized simultaneously in different points of interest, a requirement to evaluate the one-to-many encapsulation of collective measurements, a common starting point is chosen, the building of the Chair of Computational Social Science at ETH Zurich, which falls in close proximity between the two points of interest: (i) *Zurich Hauptbahnhof* that is the main station of the Zurich city center and (ii) *ETH Zurich Hauptgebaüde* that is the main building of ETH Zurich. Both groups start their navigation at the same time, i.e. mimicking two swarms. This makes the participation of the test users in the experimental process simpler. However, this localization synchronicity is an undesirable experimental artifact as in reality mobility patterns differ among citizens. To limit the synchronicity effect, each user has a localization circle with different radius value: 50, 100 or 150 meters. The circle, instead of an ellipse, is used here for simplifying the analysis and interpretability of the localization traces.

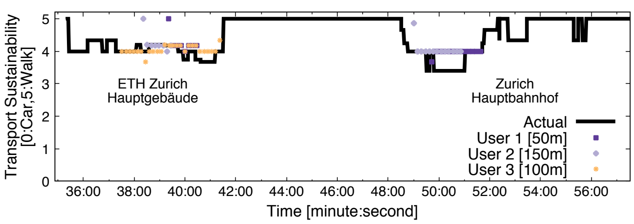
Figure 7 illustrates the accuracy of the collective measurements for each group and test user. The estimates of the average transport sustainability that each test user receives

[6]Group 1 has followed a shortcut on the way to ETH Zurich Hauptgebaüde by using the Polybahn: https://en.wikipedia.org/wiki/Polybahn (last accessed: June 2019).

approximate well the actual values. Note that users with higher localization radius receive aggregate estimates earlier and they have a larger[7] time span during which the receive collective measurements.



(a) Group 1.



(b) Group 2.

Figure 7: Accuracy of real-time collective measurements during the testnet scenario on 3.6.2019 between 13:00 and 14:00 for 6 users split in 2 groups. The aggregation function calculated is the average transport sustainability among all test users localized in one of the two point of interests of Zurich Hauptbahnhof and ETH Zurich Hauptgebaüde.

Table II shows the choices of transport means made by each test user at each point of interest. Overall, none of the more unsustainable transport means, i.e. car, bus and train, are chosen by test users to visit the points of interest. Walking and tram are the most popular means given that ETH Zurich and the main train station are very well connected with tram and are in close proximity. The mean sustainability of 4.17 for ETH Zurich Hauptgebaüde is slightly higher than the one of 3.8 at Zurich Hauptbahnhof.

Table II: Transport sustainability responses for the two points of interest.

Group	Test User	Zurich Hauptbahnhof	ETH Zurich Hauptgebaüde
1	1	5. Walking	3. Tram
1	2	3. Tram	5. Walking
1	3	5. Walking	5. Walking
2	1	3. Tram	4. Bike
2	2	3. Tram	5. Walking
2	3	4. Bike	3. Tram
	Mean:	3.8	4.17

[7]Localization circles with lower size in which test users may not remain for enough time may result in not receiving collective measurements as observed in the second group at the Zurich Hauptbahnhof point of interest.

VII. Discussion

This section discusses dynamic consensus for proving witness presence as well as the role of self-governance and artificial intelligence in the augmented democracy paradigm.

A. Dynamic Consensus and Self-governance

Proof of witness presence can be validated in a private (permissioned) or public (permissionless) network of nodes running the consensus. For instance, a legally binding decision-making process run by city authorities may require a private network of legally representative nodes, similarly to poll clerks in general elections. In case of democratic institutions that may not be well-established, a public network can be a better fit for open self-governed communities encouraging active participation. Moreover, meeting consensus performance requirements using public networks requires access to high-performing public clouds federated by communities or crowd-sourced computational resources deployed by citizens in large-scale.

An adjustable consensus cost by blockchain platforms, such as Insolar [51], involve trade-offs between transaction value vs. risk and speed vs. cost. Such adjustments can be made within community domains that determine validation rules, the number of consensus voters as well as policies/regulations for smart contract execution and data, e.g. GDPR, HER, HIPAA, EMR. Such domains can also also be used for the self-governance of the augmented democracy paradigm with blockchain providing an efficient and effective automated dispute resolution: reaching consensus on the design of a decision-making process, i.e. navigation modality and encapsulation of the collective measurements.

B. The role of artificial intelligence

Decision support systems such as digital assistants run by artificial intelligence can make decision-making more informed and efficient by overcoming the barier of expertise knowledge required to reason about a citizen's choice. However, machine learning algorithms often require sensitive personal data to operate and can be used to nudge citizens and undermine democracy [52]. For instance, the spread of fake news in social media can influence results of elections and therefore massive manipulation of democratic processes is possible using intelligent algorithms [53]. This paper distinguishes two socially responsible and ethically aligned applicability scenarios of artificial intelligence in the proposed augmented democracy paradigm: (i) *local intelligence* and (ii) *collective intelligence*.

Local intelligence concerns the use of open source machine learning algorithms that run locally at personal devices of citizens. These algorithms make use of localized or remote open data and they can be used to assist citizens in reaching complex decisions. For instance, a distributed content-based recommender algorithm for more sustainable grocery product choices can make use of public product data related to sustainability. Representation models of these product data can be computed by official authorities and environmental organizations before transferred to citizens' smart phone for personalization [54]. The limitation of local intelligence is that it assists decisions taken from an individual's perspective and it cannot address complex coordination problems that involve several citizens.

Collective intelligence can address such coordination problems, though the challenge of privacy and transparency remains subject of active research. The concept of *federated learning* is a promising approach for supervised machine learning algorithms and is based on the concept "bring the code to the data, instead of the data to the code" [55], [56]. The concept of *collective learning* is introduced for solving NP hard combinatorial optimization problems in a fully decentralizated fashion given citizens' constraints on privacy and autonomy [57]. In the augmented democracy paradigm, collective learning can address tragedy of the commons problems in which citizens' choices need to satisfy both individual and collective objectives. Collective learning has been applied[8] to combinatorial optimization problems on sharing economies, e.g. reducing demand power peaks, load-balancing of bike sharing stations, charging control of electric vehicles, traffic flow optimization and other.

VIII. Conclusion and Future Work

This paper concludes that the proposed augmented democracy paradigm is a promising endeavor for building sustainable and participatory Smart Cities. A holistic approach for augmented democracy is introduced based on three pillars that cover participatory crowd-sensing, proof of witness presence and real-time collective measurements. The Smart Agora can model a broad spectrum of collective decision-making scenarios given the different types of collected data and navigational modalities. Proving witness presence becomes a cornerstone to a more informed and responsible decision-making. It has the potential to cultivate high level of engagement and participation by reestablishing a digital revive of a cyber-physical agora, a public arena of discource and deliberation. Linking real-time collective measurements to witness presence provides an added value to crowd-sourced data analytics made by citizens, for citizens. This paper shows how blockchain consensus and crypto-economic design can realize such a grand vision by validating location proofs and incentivizing physical presence. Several localization approaches are reviewed. An experimental testnet scenario is designed and launched to provide a first technical proof of concept of the proposed augmented democracy paradigm.

Future work includes the expansion of the testnet scenario with more advanced and secure proofs of witness presence, beyond GPS. Relying on token curated registries such as the ones of FOAM [11] for the participation of test users is also subject of future work. Moreover, further use cases in conjunction with city authorities and local communities are required to assess what navigational modalities and encapsulations of collective measurements find applicability in real-world. The role of self-governance and an ethically aligned artificial intelligence are expected to play a key role in realizing augmented democracy at large-scale.

[8]EPOS, the *Economic Planning and Optimized Selections* is a realization of the collective learning concept: http://epos-net.org (last accessed: June 2019).

Acknowledgement

The author would like to thank Atif Nabi Ghulam for his development contributions in Smart Agora as well as Edward Gaere and Renato Kunz for supporting the development and deployment of the testnet scenario. The author would also like to thank the test users for their participation and feedback. Dr. Alexey Gokhberg provided the Hive interfaces to Smart Agora, while earlier author's work together with Jovan Nikolic and all nervousnet (https://www.nervousnet.ethz.ch) team members put technical foundations for this work. Moreover, the author would like to thank his 2018 students of the course "Data Science in Techno-socio-economic Systems" at ETH Zurich who used Smart Agora and provided invaluable feedback. Many thanks go to author's Empower Polis team members as well as the Institute of Science Technology and Policy (ISTP) of ETH Zurich for running the ETH Policy Challenge and providing a venue to cultivate ideas for a digital democracy. Finally, the author would like to heartily thank Prof. Dr. Dirk Helbing and the Professorship of Computational Social Science at ETH Zurich for encouraging and supporting this research.

Appendix

References

[1] P. Salesses, K. Schechtner, and C. A. Hidalgo, "The collaborative image of the city: mapping the inequality of urban perception," *PloS one*, vol. 8, no. 7, p. e68400, 2013.

[2] S. Vosoughi, D. Roy, and S. Aral, "The spread of true and false news online," *Science*, vol. 359, no. 6380, pp. 1146–1151, 2018.

[3] D. M. Lazer, M. A. Baum, Y. Benkler, A. J. Berinsky, K. M. Greenhill, F. Menczer, M. J. Metzger, B. Nyhan, G. Pennycook, D. Rothschild *et al.*, "The science of fake news," *Science*, vol. 359, no. 6380, pp. 1094–1096, 2018.

[4] A. Fung, "Putting the public back into governance: The challenges of citizen participation and its future," *Public Administration Review*, vol. 75, no. 4, pp. 513–522, 2015.

[5] J. P. Gibson, R. Krimmer, V. Teague, and J. Pomares, "A review of e-voting: the past, present and future," *Annals of Telecommunications*, vol. 71, no. 7-8, pp. 279–286, 2016.

[6] L. LeDuc, "Referendums and deliberative democracy," *Electoral studies*, vol. 38, pp. 139–148, 2015.

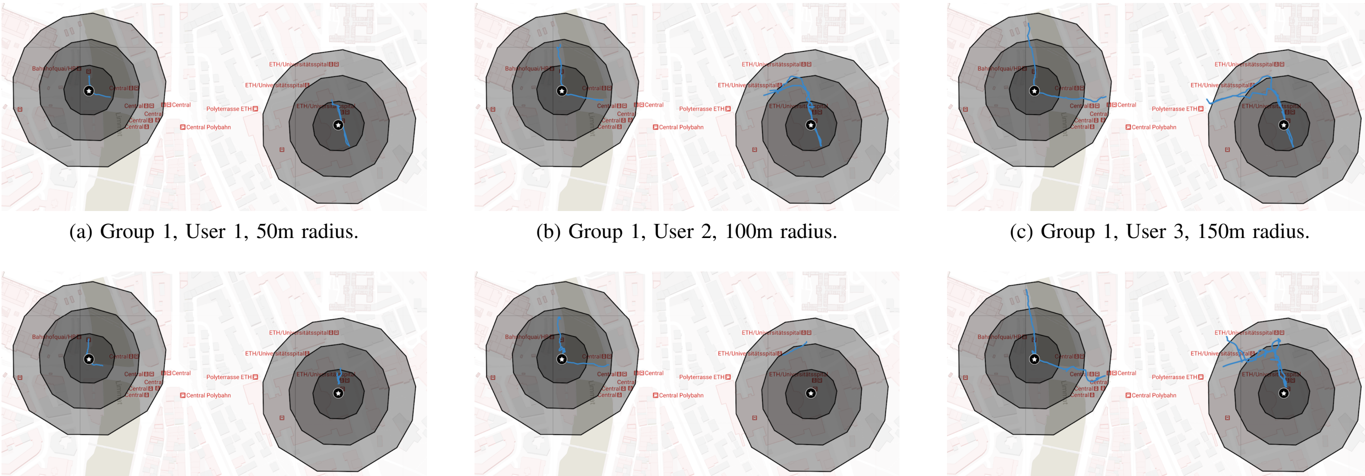
[7] M. Grčar, D. Cherepnalkoski, I. Mozetič, and P. K. Novak, "Stance and influence of twitter users regarding the brexit referendum," *Computational social networks*, vol. 4, no. 1, p. 6, 2017.

[8] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful gps spoofing attacks," in *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011, pp. 75–86.

[9] B. Nissen, L. Pschetz, D. Murray-Rust, H. Mehrpouya, S. Oosthuizen, and C. Speed, "Geocoin: Supporting ideation and collaborative design with smart contracts," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 2018, p. 163.

[10] D. Griego, V. Buff, E. Hayoz, I. Moise, and E. Pournaras, "Sensing and mining urban qualities in smart cities," in *2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*. IEEE, 2017, pp. 1004–1011.

[11] "Foam white paper," https://www.foam.space/publicAssets-/FOAM_Whitepaper.pdf, January 2018, (last accessed: April 2019).



(a) Group 1, User 1, 50m radius.

(b) Group 1, User 2, 100m radius.

(c) Group 1, User 3, 150m radius.

(d) Group 2, User 4, 50m radius.

(e) Group 2, User 5, 100m radius.

(f) Group 2, User 6, 150m radius.

Figure 8: GPS traces of test users belonging to different group and having a different localization radius.

[12] G. S. Ramachandran, R. Radhakrishnan, and B. Krishnamachari, "Towards a decentralized data marketplace for smart cities," in *2018 IEEE International Smart Cities Conference (ISC2)*. IEEE, 2018, pp. 1–8.

[13] B. H. Falk and G. Tsoukalas, "Token weighted crowdsourcing," Working Paper, Tech. Rep., 2018.

[14] L. Wolberger and V. Fedyukovych, "Zero knowledge proof of location–platin zk yellow paper," https://platin.io/assets/yellowpaper/Platin_Yellow_Paper_2018-11-18.pdf, 2018, (last accessed: April 2019).

[15] E. Pournaras, J. Nikolic, A. Omerzel, and D. Helbing, "Engineering democratization in internet of things data analytics," in *2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*. IEEE, 2017, pp. 994–1003.

[16] B. Lam, Y. P. Chen, J. Whittle, J. Binner, and T. Lawlor-Wright, "Better service design for greater civic engagement," *The Design Journal*, vol. 18, no. 1, pp. 31–55, 2015.

[17] C. Nevejan, "Witnessed presence and the yutpa framework." *PsychNology Journal*, vol. 7, no. 1, 2009.

[18] F. Musciotto, S. Delpriori, P. Castagno, and E. Pournaras, "Mining social interactions in privacy-preserving temporal networks," in *Proceedings of the 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*. IEEE Press, 2016, pp. 1103–1110.

[19] L. Chen, S. Thombre, K. Järvinen, E. S. Lohan, A. Alén-Savikko, H. Leppäkoski, M. Z. H. Bhuiyan, S. Bu-Pasha, G. N. Ferrara, S. Honkala *et al.*, "Robustness, security and privacy in location-based services for future iot: A survey," *IEEE Access*, vol. 5, pp. 8956–8977, 2017.

[20] M. R. Malekpour, "A self-stabilizing hybrid fault-tolerant synchronization protocol," in *2015 IEEE Aerospace Conference*. IEEE, 2015, pp. 1–11.

[21] ——, "An autonomous distributed fault-tolerant local positioning system," 2017.

[22] F. Victor and S. Zickau, "Geofences on the blockchain: Enabling decentralized location-based services," in *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*. IEEE, 2018, pp. 97–104.

[23] M. Amoretti, G. Brambilla, F. Medioli, and F. Zanichelli, "Blockchain-based proof of location," in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, July 2018, pp. 146–153.

[24] I. Agadakos, J. Polakis, and G. Portokalidis, "Techu: Open and privacy-preserving crowdsourced gps for the masses," in *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, 2017, pp. 475–487.

[25] F. Yucel and E. Bulut, "Clustered crowd gps for privacy valuing active localization," *IEEE Access*, vol. 6, pp. 23 213–23 221, 2018.

[26] "Platin: Proof of location blockchain - white paper," https://platin.io/assets/whitepaper/Platin_Whitepaper_v3.01.pdf, April 2019, (last accessed: April 2019).

[27] T. Dasu, Y. Kanza, and D. Srivastava, "Unchain your blockchain," in *Proc. Symposium on Foundations and Applications of Blockchain*, vol. 1, 2018, pp. 16–23.

[28] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 855–873, 2017.

[29] "The things network," https://www.thethingsnetwork.org, (last accessed: April 2019).

[30] C. Javali, G. Revadigar, K. B. Rasmussen, W. Hu, and S. Jha, "I am alice, i was in wonderland: secure location proof generation and verification protocol," in *2016 IEEE 41st conference on local computer networks (LCN)*. IEEE, 2016, pp. 477–485.

[31] R. Khan, S. Zawoad, M. M. Haque, and R. Hasan, "who, when, and where?location proof assertion for mobile devices," in *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer, 2014, pp. 146–162.

[32] Y. Li, L. Zhou, H. Zhu, and L. Sun, "Privacy-preserving location proof for securing large-scale database-driven cognitive radio networks," *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 563–571, 2016.

[33] Z. Zhu and G. Cao, "Toward privacy preserving and collusion resistance in a location proof updating system," *IEEE Transactions on Mobile Computing*, vol. 12, no. 1, pp. 51–64, 2013.

[34] C. Lyu, A. Pande, X. Wang, J. Zhu, D. Gu, and P. Mohapatra, "Clip: Continuous location integrity and provenance for mobile phones," in *2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems*. IEEE, 2015, pp. 172–180.

[35] K. D. Haggerty and M. Samatas, *Surveillance and democracy*. Routledge, 2010.

[36] J. Rouillard, "Contextual qr codes," in *2008 The Third International Multi-Conference on Computing in the Global Information Technology (iccgi 2008)*. IEEE, 2008, pp. 50–55.

[37] "Sikorka - proof of presence," http://sikorka.io, (last accessed: April 2019).

[38] K. Beckers and S. Pape, "A serious game for eliciting social engineering security requirements," in *2016 IEEE 24th International Requirements Engineering Conference (RE)*. IEEE, 2016, pp. 16–25.

[39] D. Aladawy, K. Beckers, and S. Pape, "Persuaded: Fighting social engineering attacks with a serious game," in *International Conference on Trust and Privacy in Digital Business*. Springer, 2018, pp. 103–118.

[40] P. Schaab, K. Beckers, and S. Pape, "Social engineering defence mechanisms and counteracting training strategies," *Information & Computer Security*, vol. 25, no. 2, pp. 206–222, 2017.

[41] M. C. Ugwu, I. U. Okpala, C. I. Oham, and C. I. Nwakanma, "A tiered blockchain framework for vehicular forensics," *International Journal of Network Security & Its Applications (IJNSA) Vol*, vol. 10, 2018.

[42] A. Nieto, R. Rios, and J. Lopez, "Iot-forensics meets privacy: towards cooperative digital investigations," *Sensors*, vol. 18, no. 2, p. 492, 2018.
[43] S. D. Fisher and R. Shorrocks, "Collective failure? lessons from combining forecasts for the uk's referendum on eu membership," *Journal of Elections, Public Opinion and Parties*, vol. 28, no. 1, pp. 59–77, 2018.
[44] A. Bielenberg, L. Helm, A. Gentilucci, D. Stefanescu, and H. Zhang, "The growth of diaspora-a decentralized online social network in the wild," in *2012 Proceedings IEEE INFOCOM Workshops*. IEEE, 2012, pp. 13–18.
[45] E. Pournaras, J. Nikolic, A. Omerzel, and D. Helbing, "Engineering democratization in internet of things data analytics," in *2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*. IEEE, 2017, pp. 994–1003.
[46] E. Pournaras and J. Nikolić, "Self-corrective dynamic networks via decentralized reverse computations," in *2017 IEEE International Conference on Autonomic Computing (ICAC)*. IEEE, 2017, pp. 11–20.
[47] ——, "On-demand self-adaptive data analytics in large-scale decentralized networks," in *2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)*. IEEE, 2017, pp. 1–10.
[48] E. Pournaras, E. Gaere, R. Kunz, and A. N. Ghulam, "Democratizing data analytics: Crowd-sourcing decentralized collective measurements," in *13th International Conference on Self-adaptive and Self-organizing Systems (SASO 2019)*. IEEE, 2019.
[49] M. Danaf, B. Atasoy, C. L. De Azevedo, J. Ding-Mastera, M. Abou-Zeid, N. Cox, F. Zhao, and M. Ben-Akiva, "Context-aware stated preferences with smartphone-based travel surveys," *Journal of Choice Modelling*, 2019.
[50] A. C. Prelipcean, G. Gidófalvi, and Y. O. Susilo, "Meili: A travel diary collection, annotation and automation system," *Computers, Environment and Urban Systems*, vol. 70, pp. 24–34, 2018.
[51] A. Tara, K. Ivkushkin, A. Butean, and H. Turesson, "The evolution of blockchain virtual machine architecture towards an enterprise usage perspective," in *Computer Science On-line Conference*. Springer, 2019, pp. 370–379.
[52] D. Helbing, B. S. Frey, G. Gigerenzer, E. Hafen, M. Hagner, Y. Hofstetter, J. Van Den Hoven, R. V. Zicari, and A. Zwitter, "Will democracy survive big data and artificial intelligence?" in *Towards Digital Enlightenment*. Springer, 2019, pp. 73–98.
[53] H. Allcott and M. Gentzkow, "Social media and fake news in the 2016 election," *Journal of economic perspectives*, vol. 31, no. 2, pp. 211–36, 2017.
[54] J. Klinglmayr, B. Bergmair, M. A. Klaffenböck, L. Hörmann, and E. Pournaras, "Sustainable consumerism via context-aware shopping," *International Journal of Distributed Systems and Technologies (IJDST)*, vol. 8, no. 4, pp. 54–72, 2017.
[55] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. Kiddon, J. Konecny, S. Mazzocchi, H. B. McMahan *et al.*, "Towards federated learning at scale: System design," *arXiv preprint arXiv:1902.01046*, 2019.
[56] H. B. McMahan, E. Moore, D. Ramage, S. Hampson *et al.*, "Communication-efficient learning of deep networks from decentralized data," *arXiv preprint arXiv:1602.05629*, 2016.
[57] E. Pournaras, P. Pilgerstorfer, and T. Asikis, "Decentralized collective learning for self-managed sharing economies," *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, vol. 13, no. 2, p. 10, 2018.