

очередная запись в регистр или нет, она обеспечивает уровень прозрачности и постоянства, недоступный для традиционных способов голосования.

Разработка электронной системы голосования на основе технологии блокчейн позволило бы обеспечить прозрачность выборов, конфиденциальность информации избирателей, а также полную неприкосновенность и безопасность данных. Технология блокчейн обладает всеми характеристиками, которые общественность ожидает получить от платформы, которая, возможно, является самой важной частью демократического общества.

Список использованных источников:

1. Andrew Barnes, Digital Voting with the use of Blockchain Technology
2. Roger Wattenhofer, The Science of the Blockchain : 2016
3. Springall, D., Security Analysis of the Estonian Internet Voting System : <https://jhalderm.com/pub/papers/ivoting-ccs14.pdf> : 25 сент. 2016

ПЕРЕНОС ОБУЧЕНИЯ ДЛЯ СВЕРТОЧНЫХ НЕЙРОННЫХ СЕТЕЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Гаврилович Ю.А.

Кобяк И.П. – к.т.н., доцент

Современные глубокие нейронные сети обладают интересным феноменом: будучи натренированными на большом количестве изображений, они все на первых слоях «выучивают» одинаковые шаблоны-фильтры или по-другому одинаковые приметы/признаки – простые линии, градиенты, углы, цветные пятна округлой формы. Присутствуют эти фильтры настолько часто, что отсутствие их при обучении нейронных сетей на не синтезированных наборах изображений у опытных разработчиков вызывает подозрения в программных ошибках при разработке или обучении сети. Феномен проявляется на задачах обучения как с учителем, так и без.

Т.к. похоже, что нахождение/изучение таких одинаковых примет на начальных слоях нейронной сети не зависит от типа функции потерь (lossfunction) или от типа натурального (не синтетического) набора данных, то можно называть такие приметы *общими*. С другой стороны, мы знаем, что приметы, выученные на последних слоях натренированной сети, очень сильно зависят от используемого набора данных. Например, в сети с N-мерным выходным softmax слоем, которая была натренирована на задаче классификации с учителем, каждый выходной узел будет специфичным для соответственного класса. Таким образом, приметы, выученные на последних слоях, можно называть *специфическими*.

Наличие *общих* и *специфических* примет так же хорошо согласуется с идеей иерархического обучения представлению, которая отражается в принципе работы глубоких нейронных сетей.

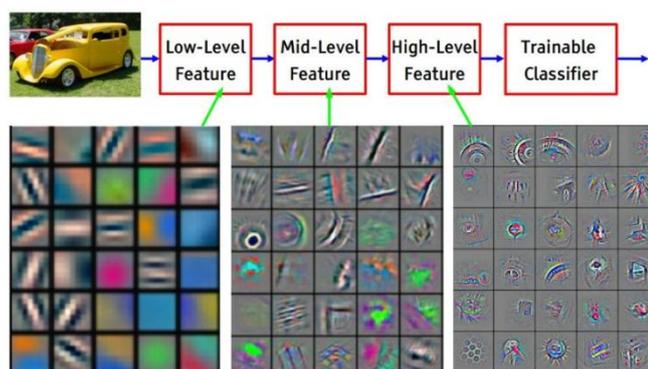


Рис. 1 – градация выученных фильтров от общих до специфических [1]

Почему нас интересует наличие *общих* или *специфических* примет? Потому, что если в процессе обучения нейронной сети можно выделить набор общих признаков, то далее мы можем использовать эти признаки для так называемого *переноса обучения* или *transfer learning* [2]. Для переноса обучения мы сначала тренируем *базовую* сеть на базовом наборе данных, затем мы переиспользуем выученные признаки, перенося их на вторую *целевую* сеть, после чего дообучиваем ее на целевых данных и целевой задаче. Такой процесс будет работать, если признаки для переноса являются *общими*, а не *специфическими*, т.е. подходят для решения как базовой, так и целевой задачи.

Если целевой набор данных значительно меньше базового, перенос обучения может быть мощным инструментом для обучения большой целевой сети без эффекта переобучения. Данная техника позволяет добиваться действительно впечатляющих результатов [3].

Типичный подход применения переноса обучения заключается в том, чтобы обучить базовую сеть, затем скопировать n первых слоев базовой сети и использовать их как n первых слоев целевой сети. Оставшиеся слои целевой сети инициализируются случайным образом и дотренировываются на целевой задаче. Так же в зависимости от ситуации можно либо «заморозить» n первых слоев в процессе дальнейшего дообучения, либо распространять ошибки обучения и на них. Такой процесс называется *fine-tuning*.

Список использованных источников:

1. Visualizing and Understanding Convolutional Networks [Электронный ресурс] : Cornell University - Электронные данные. – Режим доступа: <https://arxiv.org/abs/1311.2901>
2. Deep Learning of Representations for Unsupervised and Transfer Learning [Электронный ресурс] : Bengio et al. / Workshop on Unsupervised and Transfer Learning - Электронные данные. – Режим доступа: <http://proceedings.mlr.press/v27/bengio12a/bengio12a.pdf>
3. DeCAF: A Deep Convolutional Activation Feature for Generic Visual Recognition Networks [Электронный ресурс] : UC Donahue et al. / Berkeley. – Электронные данные. – Режим доступа: <http://proceedings.mlr.press/v32/donahue14.pdf>

БЛОКЧЕЙН КАК ОСНОВА ЗАЩИЩЕННЫХ РАСПРЕДЕЛЕННЫХ БАЗ ДАННЫХ

УО Белорусский Государственный Университет Информатики и Радиоэлектроники
г. Минск, Республика Беларусь

Глоба А.А.

Ганжа В.А. – к. физ.-мат. н., доцент

В настоящее время в связи с ростом числа пользователей Интернет-сервисов растёт и потребность в принципиально новом способе хранения данных, защищённом от атак и легко масштабируемом по горизонтали. Отличным кандидатом на эту роль может стать технология блокчейн.

Блокчейн в общем виде – это выстроенная в соответствии с определенными правилами цепочка блоков, содержащих какую-либо информацию. Обычно копии цепочек хранятся распределённо на разных устройствах в пределах одной сети. Для записи нового блока, необходимо последовательное считывание информации о старых блоках, при этом новый блок добавляется, если большая часть узлов в сети подтвердит, что в нем не нарушаются какие-либо заранее определенные правила. Все данные в блокчейн накапливаются и формируют постоянно дополняемую базу данных. С этой базы данных невозможно ничего удалить или провести замену/подмену блока, доступно только чтение.

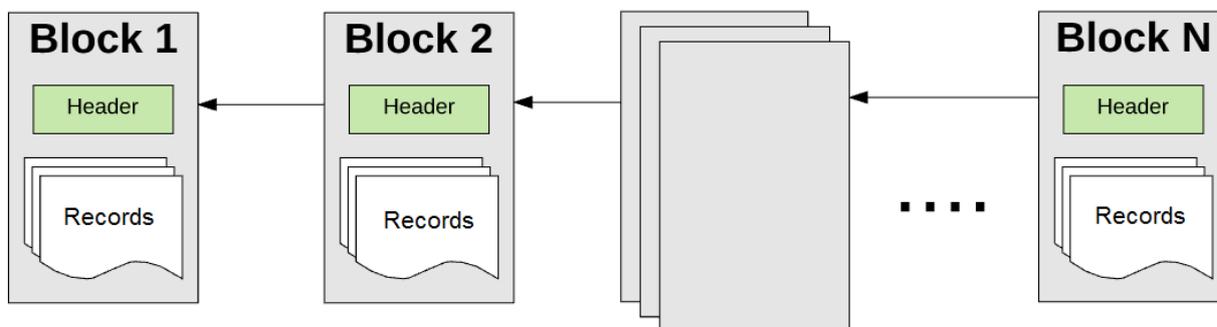


Рис. 1 – Схема блоков в БД

Главные особенности технологии блокчейн:

1. Распределенность данных: нет одного сервера, хранящего информацию. При традиционном подходе в случае какой-либо атаки на сервер или отказа оборудования по какой-либо причине теряется доступ к данным и к сервису. В случае технологии блокчейн данные распределены в виде локальных копий на разных узлах – система будет сохранять работоспособность до тех пор, пока хотя бы один узел остается в сети.
2. Невозможность изменения уже существующих данных: в случае с обычными БД всегда есть возможность преднамеренно или случайно изменить существующие записи. Сфальсифицировать новую запись можно только в том случае, если взять под контроль более 50% (если не все) узлы сети, что физически практически невозможно.

Существуют и отрицательные черты БД на основе блокчейн:

1. Низкая скорость добавления новой записи в цепочку: механизм установления консенсуса предполагает участие всех (или большинства) узлов в сети для установления соответствия нового блока правилам системы, что вызывает определенную задержку;
2. Необходимость хранения локальных копий БД: в некоторых случаях БД может разрастаться до